WSN-Enabled Privacy Preservation: A Secure Framework for Women's Data Sharing and Cyber Security in Education

A Synopsis
Submitted in Partial Fulfilment of the Requirements
for the Degree of
Doctor of Philosophy (Ph.D.) in Electronics & Communication

Submitted by:

Pallavi

Enrolment No.: JVR-II/24/040

Session: 2024-2027

Under the Supervision of:

Dr. Raj Sinha
Assistant Professor, Faculty of IT & CS, Parul Institute of Engineering and Technology, MCA, Vadodara, Gujarat

Jayoti Vidyapeeth Women's University, Jaipur, Rajasthan

NAAC Accredited |UGC Approved| Recognized by Statutory Councils

WSN-Enabled Privacy Preservation: A Secure Framework for Women's Data Sharing and Cybersecurity in Education

1. INTRODUCTION

The number of cases is rapidly growing where women on campuses at educational institutions are subject to crimes such as harassment and physical attack on women there, stirring up concerns about the safety of those students as well as women and youth in a more general sense. That said, the growing awareness has its fragility: women can be at the mercy of their surroundings, particularly at night or in dimly lit spaces such as parking lots, silent libraries and deserted hallways. These incidents of harassment and violence create an insecure environment for learning in schools [1].

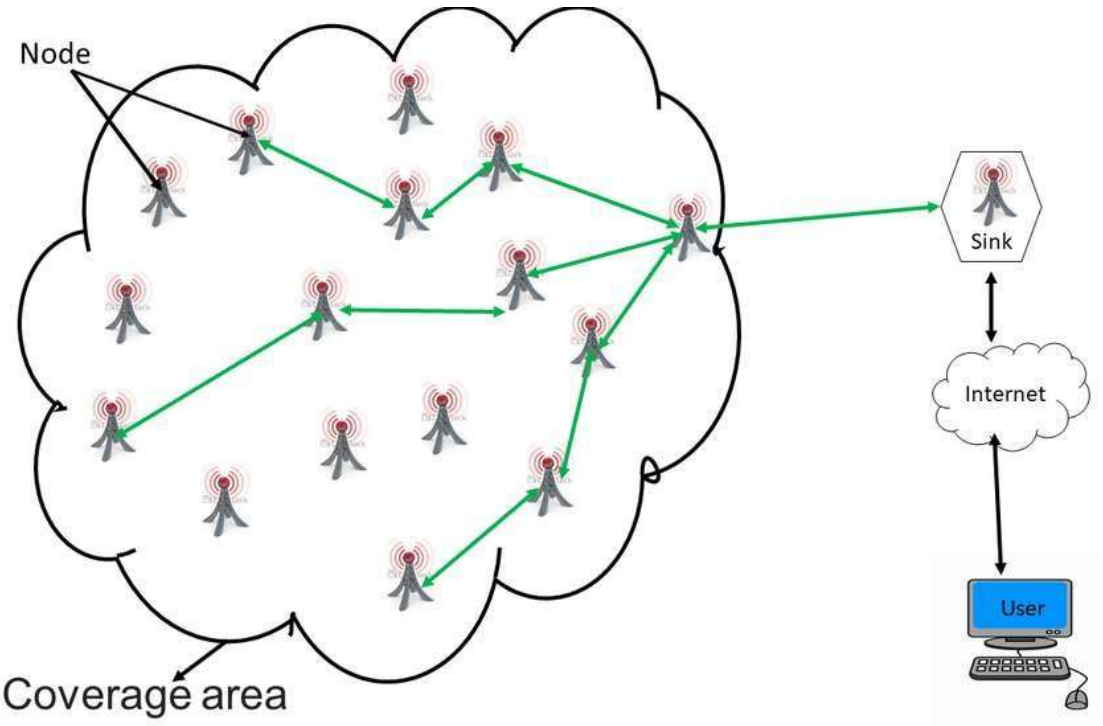

Figure 1. Wireless Sensor Network

All of these have witnessed multiple attempts to address it through various security measures on campuses, through awareness programs and others; yet as the demand for proactive solutions in real-time and the empowerment of women's safety and security continue to grow, the urgency for providing safety for the female students, staff, and

faculty grows ever greater. And with all things technology related in this new world, where you can monitor and intervene in real time, it's more important now than ever. However, while it is important for women to be safe, privacy and security of the people being surveilled must be equally considered. Combined safety surveillance systems, particularly those involving IoT devices, evoke concerns related to data privacy, surveillance, and the potential exploitation of personal data. Monitoring for women's security is often based on the premise of continuous data collection, which may relate to sensitive data such as location, physical activity and even personal health data [2]. As a result, privacy is not sufficiently protected and, in addition to being accessed by unauthorized people, it can be abused with consequences that may even affect those it is aimed to protect. It follows that those built-in safety mechanisms should be equally focused on protecting user privacy as well as the security of the data. Such encryption schemes can be applied to pseudonymize personal data. Procedures must be established that enable individuals to determine what information about them is collected and shared. So, achieving efficiency of safety in the presence of the privacy mechanism results in the development of a reliable system that shows benefit and is provably ethical [3].

The Internet of Things (IoT) [4] provides a new interface for people to engage with the environment by bringing many connections to those objects that assist in gathering, processing and disseminating data about the immediate environments. For women's safety in educational institutions, Iot can help in observing any situation with real time and even intervene. Wearable sensors such as those built into smartwatches or fitness trackers are a solid sort of safety monitor system. These gadgets can monitor the wearers' physical activities, heart rates, and GPS locations to detect anomalous behaviors or

scenarios that might be making them worrying. If a woman falls down, starts running, or exhibits signs of distress or danger, the system will immediately alert campus security or trusted contacts. To process and categorize a number of human activities into a specific activity based on the data collected from sensors, activity recognition has been a must-have prerequisite. applications that involve activities recognition and classification, of if a user is walking, running, sitting, or falling, as in these use cases, deep models such as spatial feature extraction models using CNN networks and analysis on temporal patterns based on LSTM networks may be used. This would enable campuses to connect wearable sensors and sophisticated activity detection to the Internet of Things, completing the safety monitoring system in the aspect of real-time threat detection while preserving privacy. As such, it gives these technologies a new context in which to effectively improve campus security while giving women peace of mind about their personal data and autonomy.

Significance of the Research

This is very important as it deals with the design of a privacy-preserving cyber-security framework for safety monitoring at school campuses, which is one of the pressing challenges of the contemporary world and is related to many converging topics for example women safety, data privacy, and technology advancement. The past few years have even seen such cases within educational campuses, turning into calls for more proactive, real-time measures that can start responding to threats related to privacy and personal boundaries. This research fulfills the immediate short-term requirements of guaranteeing safety in campus for all and the long-run needs of protecting privacy in an ever digitizing world as it proposes a solution that integrates wearable sensors with a hybrid deep learning model in [5].

It has the potential to significantly improve the safety of women in schools. It provides a means to monitor activity and detect early signs of potential threats like harassment or physical trauma from wearable sensors, and confirms that undesired events are identified and handled in a timely manner. This would have a positive impact on the lives of numerous women as it will prevent them from being victimized by sexual assault in educational institutes, as well as in whole areas, largely in these kinds of situations. Apart from that, the study has a part to play in privacy in safety systems. Wearables and IoT solutions have more traction, but there is a deep sensitivity around the value of that data. Hence, in this study a framework has been proposed which is also privacy-preserving so that safety does not trespass into personal lives. And this is presumably a problem for a lot of users of security monitoring technology: If you have people feeling like they're being harvested for their data, it could be rough both from the standpoint of adoption and usage. In this approach, a person's sensitive data is anonymized and encrypted, and it is accessed solely for the specific application of ensuring safety. This has allowed for better user confidence and system adoption [6].

Due to the recent advances in deep learning techniques mainly formed by hybrid approach of Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) units, there is a new paradigm of human activity recognition. This may mean enabling the precise identification and categorization of the activity being performed, followed by differentiating between safe and unsafe actions. This is very basic especially for real-time monitoring system. The activity data now has to make haste and snap judgement. In this paper, the boundary of cloud computing broadens a bit more beyond the one customized in the IoT-based security systems.

This also accounts, when taken from another perspective, to the be the fast growing area of privacy-preserving and security-aware cyberinfrastructure. From now on, this will be translated as IoT + wearables x deep learning = stream innovations for the future in privacy-aware systems that could be evolved security-wise and applied not only women's safety but healthcare, personal security or smart city applications. The proposed approach and techniques can also be applied to other scenarios where privacy-preserving real-time surveillance is critical.

Finally, this research will be significant to the learning institution because it will promote the safety of women in this learning environment with the highest standards of privacy and data security. It is hence a forward-looking solution that will look forward to embracing all the promises that technology holds to create safer learning environments still respecting the rights of people.

2. RESEARCH AIMS AND OBJECTIVES

2.1 Research Aims

The main goal of this research is to design and implement a privacy-preserving cybersecurity framework for women's safety monitoring in educational campuses by utilizing the power of Internet of Things (IoT) technologies, wearable sensors, and advanced deep learning models. The developed system should be able to monitor women's activities in real time. It would therefore serve as a basis for immediately detecting and responding to potential threats, such as harassment, falls, or other forms of distress, while concealing the privacy of those involved. Thus, combining these advanced technologies in the proposed research will bridge the gap between enhanced campus safety and personal data privacy concerns.

The work of developing a hybrid deep learning model is part of this research. The proposed hybrid deep learning model is expected to incorporate the advantages of both Convolutional Neural Networks (CNNs) for spatial feature extraction and Long Short-Term Memory (LSTM) networks in capturing temporal dependencies of human activity. This shall be an accuracy system for predefined activities like walking, sitting, standing, or even falling, in real-time classification by using data acquired from wearable inertial sensors. These are examples of normal behaviours and safety hazards, and their distinctions should be made promptly in real time to allow the intervention of any distress or danger.An established Human Activity Recognition dataset will be used for model training and testing purposes, as well as pre-processed techniques that improve the quality of sensor data and reduce noise, which can degrade system performance. Another significant objective of the research is to integrate privacy-preserving

techniques into the design of the safety monitoring system.Since the data collected by the wearable sensors are sensitive in nature, such as personal location, health metrics, and physical activity, it is crucial that all collected data be treated with security. Through these anonymization and encryption methods for protecting personal data, the project guarantees that the monitoring data used, although collected during the safety inspection stage, will have integrity from misuse and leakages. Furthermore, by looking into privacy as a concern on one hand, such a system's result is expected to be effective as it enhances users' safety experience and trusted through privacy protection features it incorporates.

Moreover, this research will investigate the proof-of-concept real-world integration of such a system into existing IoT infrastructures on educational campuses. A framework that could communicate with current campus security systems should be designed to allow for quick responses to alerts generated by the safety monitoring system, notifying campus security officers, emergency responders, or specific safety contacts about threats and emergencies detected by the system.The development of a scalable and portable solution applicable to any school is the main focus of the work, with the system being made to fit within the overall campus security architecture. One purpose of the research is to evaluate the proposed system's performance in real situations, however, it will take place as a simulation application.In this respect, the application will be run on a simulated campus while the accuracy of activity and threat detection when running the application will be evaluated as well as the capability of protecting user privacy.The outcomes of these evaluations will provide valuable insights into the potential for such systems to be deployed on campuses and to identify needs for further improvement or development.

To summarize, this work focuses on designing and prototyping an end-to-end privacy-preserving women's safety monitoring system based on IoT, wearable sensors, and advanced deep learning models. The objective is to build a system which for one is privacy-preserving in nature and detects potential information security threats in the first place, and secondly, demonstrates to a large degree the applicability of the system in the facet of users, and thus, in campus security, It opens possibilities for broader application in smart campuses in using IoT driven safety solutions.

2.2 Research Objectives

The objectives of research are as follows,

1. **To conduct an inclusive literature review:** Analyze literature regarding the women safety systems, human activity recognition, IoT privacy issue, and the deep learning approaches.
2. To design a hybrid deep-learning-based human activity recognition model Implement a CNN+LSTM combination to classify between six activities with the wearable sensors, which were: walking and sitting. Include wearable inertial sensors in monitoring systems.
3. To incorporate sensors, such as accelerometers, capable of collecting data concerning real-time, real physical activity by the user for purposes of proper monitoring.
4. To implement Privacy-preserving mechanisms within the monitoring system. Use encryption and anonymization techniques to protect sensitive data and maintain user confidentiality.

5. Hybrid model and system performance evaluation Model accuracy and effectiveness of the entire system in a real-world setting, including potential threats.
6. To evaluate the scalability and real-world integration of the system on educational campuses
7. To evaluate how well the system could be integrated with the existing security systems of a campus and whether it is scalable for wider deployment.

These goals aim to design a trustworthy, privacy-preserving system to increase women's safety on educational campuses.

2.3 Research Questions

1. Are there ways in which privacy-by-design concepts can be applied to a wearable sensor–based Human Activity Recognition (HAR) system that aims to provide women's safety on educational campuses?
2. Is it possible to employ a hybrid CNN–LSTM deep learning architecture for real-time recognition of normal and abnormal activities of the human body using data from wearable inertial sensors?
3. How can one develop a seamless platform for campus safety monitoring that encompasses WSNs, wearable devices, deep learning models, and privacy-preserving techniques?
4. What is the performance of the suggested solution in a real-time campus environment where safety-related incidents, e.g., falling or distressing events, are expected to be captured?

5. Can the proposed privacy-preserving safe monitoring system be effectively scaled and interoperated with real-world campus security systems?

3. REVIEW OF LITERATURE

Bigelli, L., et al. (2024) [7]: Energy-conscious Privacy Preserving Human Activity Recognition with Deep Learning Autoencoder. In this contribution, the authors proposed an energyaware method to protect privacy in human activity recognition systems. They deployed a deep learning autoencoder to eliminate sensitive private information (weight, height, age, gender) from sensor signals without compromising classification accuracy. It trades energy and accuracy to be suitable for low-power ARM-based platforms. Results of experiments are reported to achieve accurate-sensitive attributes obfuscation with a minor degradation (5% while consuming 165 mJ of energy and 30 ms in processing).

Ahmed, A. et al. 2024 [8]: WSNs, which is the best data processing technology for emergency response, national security, and medical care. Access control, anonymization, authentication and encryption can be used to enforce data privacy in WSNs. Part of its challenge is related to regulatory and vulnerability. In order to promote the spread of the privacy enhancing technologies in WSNs, the Diffusion of Innovation Theory could be applied, and possibly there are other suitable theories. There is a security solution could ensure the sensi- tive information are kept in WSNs as these researches show.

Akinsola, A., et al. (2024) [9]. Privacy-preserving Techniques in WSNs: encryption, access control. It also investigates the diffusion of innovation theory regarding the adoption of P-ETs, and examines research on protecting data privacy in WSNs, summarizing developments in sensitive data safeguarding.

Masood, A., et al. (2023) [10]: In this paper, an approach to a privacy-preserving healthcare application utilizing WSNs is proposed. The method combines multipath routing with the secret key concepts such as the confidentiality of the data during transmission is maintained. The algorithm finds the best route for data secured transmission using ECSO and BO. The simulation results show that secret key-based multipath routing enhances the WSN-based healthcare system privacy security as well as throughput and energy efficiency.

Moulahi, T., et al. (2023) [11]: An article on the application of federated learning (FL) for ITS of vehicles using block chain technology to ensure data integrity in the presence of privacy protection. Models produced from cars and then stack these models while preserving privacy at the time of detection of cyber threats results in 7.1% decrease in model accuracy with,F1-score, and recall are preserved with minimal gas consumption during the process of model aggregation.

Yadav, S., & Tiwari, N. (2023) [12]: Revocable identity-based broadcast encryption scheme for anonymous secure multimedia communication in group communication. In the context of this paper, we address the issue of privacy by ensuring that only legitimate users can access the transmitted content even after the revocation. It can be proved that the schemes is semantically secure against IND-ID-CPA attacks and it is computationally efficient and communication bandwidth efficient.

Chen, Z et al. 2023 [13] The MP-HAR, a motion-driven human activity identification system for the IoT platform, the authors proposed. The MP-HAR aims one to off chemical- batteries dependency and the other to energy harvesting and edge computing

toward an energy efficient and sustainable solution for HAR in IoT- based use case/application.

Beemkumar, N. et al. (2023) [14] In this research, transfer learning in deep learning models for HAR is proposed along with the problem of noisy data. This method enhanced the classification accuracy significantly, especially in image-based applications, which suggests the possibility of utilizing transfer learning to enhance HAR.

Mekruksavanich, S. & Jitpattanakul, A. (2023) [15]. In this paper, the authors review the state of the art deep learning techniques for the HAR and propose a channel attention based hybrid CNN model that exploits the best of both channels.

This subsequently gives better feature extraction, which also leads to better accuracy in classification for the improvement of deep learning based HAR system.

Vidya, B. & Sasikumar, P. (2022) [16] Supervised learning model for wearable sensor data has been created in this study by taking the advantage of Time frequency domain Analysis Techniques namely DWT and EMD. Their impressive 99.63% classification accuracy demonstrates the power of these methods for HAR.

Athota, R. K. & Sumathi, D. (2022) [17] Paper proposed hybrid learning algorithms CMFA and CGFA for HAR using IoT and wearable based devices. Using the WISDM dataset, high classification accuracies of 97.76% and 96.91% are achieved by the authors, validating the usefulness of their proposed algorithms.

S. Bian et al. (2022) [20] The authors where the summary of sensing modalities in HAR is given and then followed by the brief introduction that specific modality belongs within

the kinematic-based, field-based, wave-based, physiological and hybrid categories. In this way their works has been granted the possibility to select from a suitable HAR approach, which is application specific.

Mishra, C. S. et al 2022 [21] Submitted "Origin, an energy aware scheduling algorithm targeted at IoT platforms 2.5% better in comparison with legacy algorithm classification efficiency Usi ng the considered was con- centrated in ener- gy consumption in IoT HAR systems.

Chen, Z. et al. (2021) [22] The authors introduced HAR-SAnet, a device-free HAR scheme based on RF signals. The framework adopted shallow networks for processing time- and frequency-domain features compactly and efficiently to perform feature fusion, achieving better performance than other existing HAR models and moving forward RF-based HAR solutions.

Table 1. Literature Review Findings

Author Name (Year)	**Main Concept**	**Findings**	**Limitations**
Bigelli, L., et al. (2024)	Privacy-preserving human activity recognition system using deep learning autoencoder	Proposed an energy-aware system that obfuscates sensitive data (e.g., weight, age) with minimal accuracy loss (5%) and low energy consumption (165 mJ, 30ms).	Only minimal accuracy loss allowed, but the trade-off between privacy and accuracy may not suit all applications.

Ahmed, A., et al. (2024)	Privacy solutions in Wireless Sensor Networks (WSNs)	Discussed encryption, anonymization, and access control techniques in WSNs. Identified challenges and adoption barriers in healthcare and security applications.	The study did not explore specific privacy-enhancing technologies in detail, focusing more on concepts and theory.
Akinsola, A., et al. (2024)	Privacy and security in WSNs for healthcare and security sectors	Explored data privacy techniques in WSNs and highlighted the Diffusion of Innovation Theory in technology adoption.	Similar to Ahmed et al., did not deeply investigate specific implementations of privacy-enhancing technologies.
Masood, J. A. I. S., et al. (2023)	Privacy-preserving method for healthcare WSNs using multipath routing and secret keys	Introduced multipath routing and secret key principles with optimization techniques to secure healthcare data in WSNs, improving throughput and energy efficiency.	Requires computational resources for path optimization, and the efficiency of the method depends on network size and routing complexity.

Moulahi, T., et al. (2023)	Federated learning and blockchain for privacy in intelligent transport systems (ITS)	Applied federated learning for privacy in vehicles, ensuring data aggregation safety with blockchain, with slight accuracy loss (7.1%) in cyber-threat detection.	The trade-off between privacy and accuracy may limit real-world application, especially for critical systems where accuracy is paramount.
Yadav, S., & Tiwari, N. (2023)	Broadcast encryption for secure multimedia transmission in group communication	Developed a secure broadcast encryption scheme ensuring that only legitimate users can access content, with efficiency in computation and communication.	May not fully account for scalability in larger systems or high-demand communication environments.
Chen, Z. et al. (2023)	Motion-powered HAR system for IoT environments	MP-HAR reduces dependency on chemical batteries by leveraging energy harvesting and edge computing.	Limited exploration of scalability and adaptability to diverse IoT environments.
Beemkumar, N. et al. (2023)	Transfer learning in deep learning models for HAR	Improved classification performance in vision-based scenarios while	Limited focus on datasets beyond vision-based scenarios.

		addressing dataset noise issues.	
Mekruksavanich, S. & Jitpattanakul, A. (2023)	Hybrid CNN model with channel attention mechanisms for HAR	Enhanced feature extraction and classification accuracy through the proposed hybrid CNN model.	May require significant computational resources for real-time applications.
Vidya, B. & Sasikumar, P. (2022)	Supervised machine learning framework using time-frequency analysis (DWT, EMD) for wearable sensor data	Achieved 99.63% classification accuracy for HAR using wearable sensor data.	Focused only on wearable sensor data without addressing multimodal approaches.
Athota, R. K. & Sumathi, D. (2022)	Hybrid learning algorithms (CMFA and CGFA) for IoT and wearable-based HAR	Achieved 97.76% and 96.91% classification accuracy using WISDM dataset.	Results are dataset-specific and may not generalize well to other datasets.
Bian, S. et al. (2022)	Overview of HAR sensing modalities	Categorized HAR sensing modalities into kinematic-based, field-based, wave-based, physiological, and hybrid approaches.	Limited experimental validation of the proposed categorization framework.

Mishra, C. S., et al. (2022)	Energy-conscious scheduling algorithm ("Origin") for IoT platforms	Improved classification efficiency by 2.5% over legacy algorithms while optimizing energy usage.	Specific to certain IoT applications and lacks generalization to broader HAR systems.
Chen, Z. et al. (2021)	RF-based device-free HAR framework (HAR-SAnet)	Proposed compact neural networks for efficient time- and frequency-domain feature fusion, outperforming existing models.	Limited applicability to scenarios where RF signal interference is significant.

Research Gaps

1. Lack of privacy-by-design in HAR systems (2A)

To date, performance optimization of Human Activity Recognition (HAR) systems has been the focus of attention while privacy protection has not been taken into account from the system design layer. Sensitive data from wearable sensor data is often processed in a raw form that is unencrypted, or unanonymized.

2. No full end-to-end integrated solution

Prior works generally focus on a portion of the problem such as wearables sensors, activity recognition, or security. To the best of our knowledge, there has been no end-to-end framework that integrates wireless sensor networks (WSN), wearable devices, deep learning model and privacy preserving schemes.

3. Few Real-time On a Educational Campus

It is well-known that the majority of human activity recognition (HAR) based security systems are only tested in offline or controlled environments. The study of efficient real-time execution, system latency and campus security system infrastructure integration for real-world application is missing.

These shortcomings call for a privacy-preserving, end-to-end and real-time monitoring of a women safety system specifically designed for educational campus.

4. RESEARCH METHODOLOGY AND MATERIALS

In this research study, a systematic approach was applied that considers the data collection/model development/model integration/evaluation process, condensing each stage with the research objectives. It was divided into well-defined stages which collectively evolved and validated the proposed privacy-preserving women's safety monitoring system. A more detailed look at the methodology can be found in the following sections:

1. Literature Survey and Identification of Problem

It is preceded by a full literature survey on women s safety systems, activity recognition using wearable sensor-based wearable devices, privacy-preserving techniques, and deep learning models [23]. This would help to determine any misses in existing solutions, largely due to challenges experienced by extant safety systems on educational campuses due to inadequacies in the levels of privacy and security affordances through IoT-based systems. The development of the deep learning models and the privacy-preserving framework are motivated by the literature review results.

2. System Design and Architecture

This is the stage in which the design of safety monitoring system developed. The system will be made of a few wearable inertial sensors such as accelerometers and gyroscopes to monitor physical activities, a deep learning model represented by hybrid CNN-LSTM for recognizing activities, and privacy-preserving methods to safeguard the data. It is intended to obtain activity data in real time and to recognize up to six pre-defined activities such as walking, sitting, standing, etc. to identify unusual behavior or voluntary risk [24]. With an appropriate architecture, tight coupling of sensors with the

deep learning model results in maximum performance in the processing of data in both inflow and flow modes.

3. Data Collection and Pre-processing

The analyses/methods are Data Processing and Analysis of the Survey Using a structured questionnaire, which constitutes the primary data source, the study was conducted to understand the activity pattern of women in educational institutions, their perception of safety, risk situations they are exposed to, their response mechanism in emergency situations and the viability of wearable safety devices from their point of view. In addition to the questionnaire data, a publicly available dataset for human activity recognition (HAR) [25] with labeled sensor data for different physical activities is also used as an auxiliary dataset to support the training and testing of the hybrid CNN–LSTM model. Upon collection, the data are preprocessed for quality and consistency; survey responses are processed by cleaning and imputing missing data and converting categorical responses to dummies, while considering imputation of missing values in sensor-based data, if applicable; signals are filtered, normalized,windowed/segmented and features are extracted to improve signal quality and model performance. Techniques that preserve privacy are applied during the stage of data collection and processing, e.g., personal identifiers are anonymized and data are stored and handled securely, enabling meaningful analyses and model-building at the same time as protecting sensitive data.

4. Model Development and Training The spatial feature extraction capability of CNN and temporal dependencies extraction properties of LSTM for application of human activity are combined in an hybrid deep learning model for activity recognition. CNN is utilized to analyzenerve data and to detect latent spatial features in the neural data, and

the sequential nature of human activity is modelled using LSTMs [26]. The processed data will be utilized in model training, and the model performance will be evaluated in terms of accuracy, precision, recall, and F1-score. Then, cross-validation based hyperparameter optimization is applied to obtain better model performance.

5. Enforcement of Privacy-Protecting Mechanisms

The collection of data using wearable sensors is no longer a requirement, with privacy being protected by employing privacy-preserving [27] techniques. The information gathered will be anonymized, and appropriate encryption will be applied to sensitive information as it is transmitted and stored. To conclude, users' privacy and control over their data would be achieved via privacy-by-design implementing them from the very root. This step is to guarantee the system is data protection standards compliant and that it provides a good safety solution.

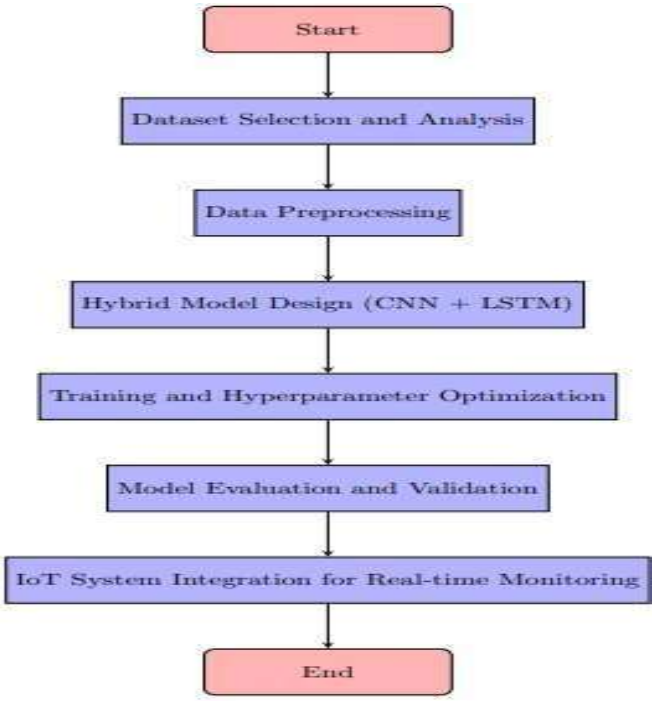

Figure 2. Research Flow Diagram

6. System Integration and Testing

An in-environment prototype that incorporates the proposed system will be designed to emulate the in vivo campus environment. The proposed combination of wearable sensors [28], deep learning model, and privacy schemes will be evaluated as a whole for the working efficiency of the system. They are now being phased in, tying the secure infrastructures into the campus There must be alerts when potential threats arise by way of responses.

7. Performance Evaluation

Once all the modules have been integrated, the proposed women safety monitoring framework will be evaluated using machine based simulations experiments rather than real campus deployment. This assessment is to confirm the accuracy and efficiency of activity identification, voyeurism recognition and alert generation in computational environment. The performance of the hybrid CNN–LSTM model will also be tested in terms of other conventional statistical classifiers, such as accuracy, precision, recall and F1-score [29]. In addition to the model accuracy, the performance of the privacy-preserving methods will also be assessed through data leakage risk analysis, quantification of the encryption and decryption overhead in terms of computation, and evaluation on the delay induced by the privacy schemes in data processing and communication. Real-time execution will be conducted in the simulation to ensure that the system detects and responds to safe incident immediately, with strong privacy guarantees. Such a testing mode does allow some assessment of system viability and performance trade-offs in even prior to any field deployment.

8. Scalability and Integration with Campus Infrastructure

The scalability of the system and its integration with campus security systems will be assessed based on the ability of the system to support a larger number of users and its compatibility with IoT infrastructure [30] that is prevalent on educational campuses. Here, the ability of the system to scale up to a real-time safety monitoring of a number of individuals scattered across a campus is discussed. Performance of the deep learning model, impact of privacy enhancing techniques, and applicability of the system in real-world will be discussed during this stage. This step also involves comparison between proposed system and existing safety monitoring solutions, in order to highlight the enhancement in terms of safety detection and data privacy.

9. Conclusion and Future Work

Implications of research will be drawn on how the proposed system fares. Enhancements, future directions and other potential applications for the system in other domains will also be considered as part of the research. Recommendations are to be made on how best the system could be optimized and extended to real-world campus scenarios. To conclude, the methodology is an end-to-end process encompassing design, data collection, modeling, privacy, and real-world evaluation of the system. It offers a systematic approach for designing a privacy preserving, IoT-based women's safety monitoring system utilizing deep learning to secure the campus with user data privacy.

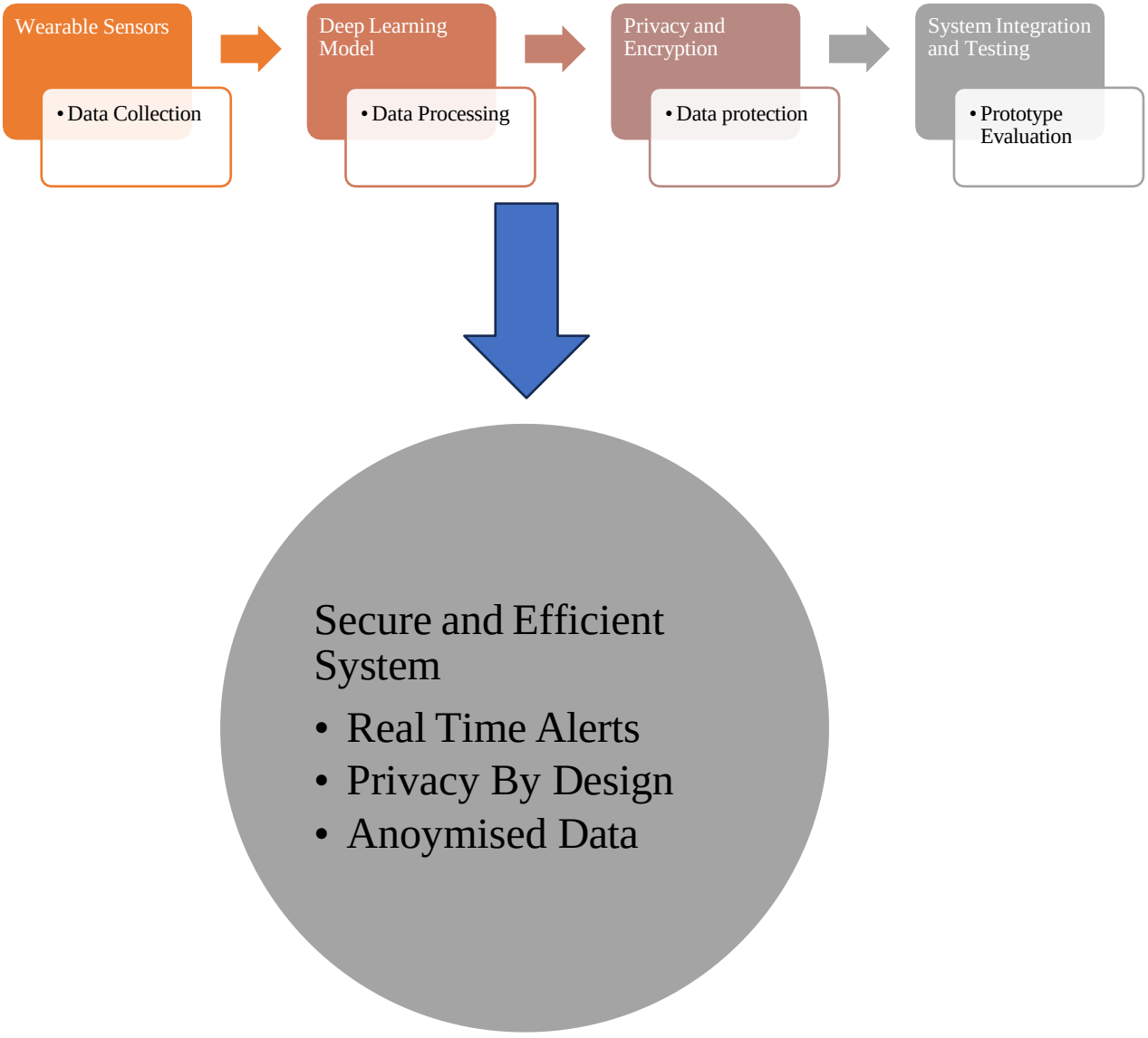

Figure 3. System Flow Diagram

Timeline Diagram:

Phases	**1-6 Months**	**7-12 Months**	**13-18 Months**	**19-24 Months**	**25-30 Months**	**31-36 Months**
Phase I	Define Research Objectives and Questions Conduct a Comprehensive Literature Review Synthesize and Analyze Literature					
Phase II		Select Research Methodology Data Collection Initial Data Analysis and Method Refinement				
Phase III			Model Selection			

			Model Training Model Evaluation			
Phase IV				Testing and Optimization Integration		
Phase V					External Validation Results Analysis Manuscript Preparation	
Phase VI						Thesis writing and submission

5. EXPECTED OUTCOME OF THE PROPOSED WORK

The output to be generated from this research is a more robust and privacy-secure system for w-monitoring women safety that involves wearable sensors, deep learning models, and real-time activity recognition. It can classify the correct activities such as walking, sitting, standing and so on predefined behaviors with high accuracy, so it can detect unusual or even dangerous activities that may include falling down or sending distress signals. It will be a mixed deep learning model employing CNNs for spatial features extraction and LSTM networks for temporal dependencies modeling, and providing high accuracy and real-time performance as well. User trust and compliance with data protection laws would be enforced by implementing privacy-preserving techniques (e.g., data encryption and anonymization of sensitive data). It's designed to be multi-user scalable, so it could be deployed on larger educational campuses without a hitch. It also interfaces with other campus security systems, allowing for the dissemination of alerts for potential security threats to security officer or emergency responder on the scene. Such integration can represent the whole campus security system as a whole, and provide a consistent solution for monitoring and responding to safety threats. The research makes a contribution as it assists in closing the gap on IoT-based safety systems with respect to privacy-preserving policies and activity recognition, and the same can be extended to other areas such as healthcare and elder care. This would be an attempt to design a safe, privacy-aware and scalable system which would help in making education campus a safer place for women and at the same time act as a ground for further research in both security technologies and privacy protection.

8. REFERENCES

1. A. Saha, S. Rajak, J. Saha, and C. Chowdhury, "A survey of machine learning and meta-heuristics approaches for sensor-based human activity recognition systems," *Journal of Ambient Intelligence and Humanized Computing*, vol. 15, no. 1, pp. 29–56, 2024.
2. Q. Xie, K. Li, X. Tan, L. Han, W. Tang, and B. Hu, "A secure and privacy-preserving authentication protocol for wireless sensor networks in smart city," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, no. 1, p. 119, 2021.
3. M. G. Moghaddam, A. A. N. Shirehjini, and S. Shirmohammadi, "A WiFi-based method for recognizing fine-grained multiple-subject human activities," *IEEE Transactions on Instrumentation and Measurement*, vol. 72, pp. 1–13, 2023.
4. H. Y. Ghafoor, R. Jahangir, A. Jaffar, R. Alroobaea, O. Saidani, and F. Alhayan, "Sensors-based human activity recognition using hybrid features and deep capsule network," *IEEE Sensors Journal*, 2024.
5. Khalid, N., Qayyum, A., Bilal, M., Al-Fuqaha, A., & Qadir, J. (2023). Privacy-preserving artificial intelligence in healthcare: Techniques and applications. *Computers in Biology and Medicine, 158*, 106848.
6. Krishna, K., Bodduna Srinivas, V., & SK, K. K. V. B. (2023). WIRELESS SENSOR NETWORK-BASED RESEARCH ON COMPUTER NETWORK INFORMATION SECURITY PROBLEMS AND PREVENTION. *MATERIAL SCIENCE*, *22*(11).

7. Bigelli, L., Contoli, C., Freschi, V., & Lattanzi, E. (2024). Privacy preservation in sensor-based Human Activity Recognition through autoencoders for low-power IoT devices. *Internet of Things*, *26*, 101189.
8. Ahmed, A., Oluomachi, E., Abdullah, A., & Tochukwu, N. (2024). Enhancing Data Privacy In Wireless Sensor Networks: Investigating Techniques And Protocols To Protect Privacy Of Data Transmitted Over Wireless Sensor Networks In Critical Applications Of Healthcare And National Security. *arXiv preprint arXiv:2404.11388*.
9. Akinsola, A., Njoku, T. K., Ejiofor, O., & Akinde, A. (2024). Enhancing Data Privacy In Wireless Sensor Networks: Investigating Techniques And Protocols To Protect Privacy Of Data Transmitted Over Wireless Sensor Networks In Critical Applications Of Healthcare And National Security. *International Journal of Network Security & Its Applications (IJNSA) Vol*, *16*.
10. Masood, J. A. I. S., Jeyaselvi, M., Senthamarai, N., Koteswari, S., Sathya, M., & Chakravarthy, N. K. (2023). Privacy preservation in wireless sensor network using energy efficient multipath routing for healthcare data. *Measurement: Sensors*, *29*, 100867.
11. Moulahi, T., Jabbar, R., Alabdulatif, A., Abbas, S., El Khediri, S., Zidi, S., & Rizwan, M. (2023). Privacy-preserving federated learning cyber-threat detection for intelligent transport systems with blockchain-based security. *Expert Systems*, *40*(5), e13103.
12. Yadav, S., & Tiwari, N. (2023). Privacy preserving data sharing method for social media platforms. *PloS one*, *18*(1), e0280182.

13. R. S. Gargees, "Improving Human Activity Recognition Through Multisensor Data Fusion Techniques in Wireless Sensor Networks," in *2024 IEEE 3rd International Conference on Computing and Machine Intelligence (ICMI)*, Apr. 2024, pp. 1–5.

14. E. El-Adawi, E. Essa, M. Handosa, and S. Elmougy, "Wireless body area sensor networks based human activity recognition using deep learning," *Scientific Reports*, vol. 14, no. 1, p. 2702, 2024.

15. Z. Chen, L. Teng, L. Xu, J. Yu, and J. Liang, "MP-HAR: A novel motion-powered real-time human activity recognition system," *IEEE Internet of Things Journal*, 2023.

16. N. Beemkumar, S. Gupta, S. Yadav, A. K. Saxena, D. Dhabliya, and A. Gupta, "The Application of WSN during Human Activity Detection and Identification Using a Deep Learning Approach," in *Digital Transformation–Modernization and Optimization of Wireless Networks*, vol. 59, 2023.

17. S. Mekruksavanich and A. Jitpattanakul, "Hybrid convolution neural network with channel attention mechanism for sensor-based human activity recognition," *Scientific Reports*, vol. 13, no. 1, p. 12067, 2023.

18. B. Vidya and P. Sasikumar, "Wearable multi-sensor data fusion approach for human activity recognition using machine learning algorithms," *Sensors and Actuators A: Physical*, vol. 341, p. 113557, 2022.

19. R. K. Athota and D. Sumathi, "Human activity recognition based on hybrid learning algorithm for wearable sensor data," *Measurement: Sensors*, vol. 24, p. 100512, 2022.

20. S. Bian, M. Liu, B. Zhou, and P. Lukowicz, "The state-of-the-art sensing techniques in human activity recognition: A survey," *Sensors*, vol. 22, no. 12, p. 4596, 2022.

21. C. S. Mishra, J. Sampson, M. T. Kandemir, and V. Narayanan, "Origin: Enabling on-device intelligence for human activity recognition using energy harvesting

wireless sensor networks," in *2021 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Feb. 2021, pp. 1414–1419.

22. Z. Chen, C. Cai, T. Zheng, J. Luo, J. Xiong, and X. Wang, "RF-based human activity recognition using signal adapted convolutional neural network," *IEEE Transactions on Mobile Computing*, vol. 22, no. 1, pp. 487–499, 2021.

23. D. Rangwani, D. Sadhukhan, S. Ray, M. K. Khan, and M. Dasgupta, "An improved privacy-preserving remote user authentication scheme for agricultural wireless sensor network," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 3, p. e4218, 2021.

24. W. Guo, S. Yamagishi, and L. Jing, "Human Activity Recognition via Wi-Fi and Inertial Sensors with Machine Learning," *IEEE Access*, 2024.

25. Q. Xie, Z. Ding, and B. Hu, "A secure and privacy-preserving three-factor anonymous authentication scheme for wireless sensor networks in Internet of Things," *Security and Communication Networks*, vol. 2021, no. 1, p. 4799223, 2021.

26. P. Kumar, S. Chauhan, and L. K. Awasthi, "Human activity recognition (HAR) using deep learning: Review, methodologies, progress and future research directions," *Archives of Computational Methods in Engineering*, vol. 31, no. 1, pp. 179–219, 2024.

27. R. Priyadarshi, "Exploring machine learning solutions for overcoming challenges in IoT-based wireless sensor network routing: a comprehensive review," *Wireless Networks*, pp. 1–27, 2024.

28. O. A. Khashan, N. M. Khafajah, W. Alomoush, and M. Alshinwan, "Innovative energy-efficient proxy re-encryption for secure data exchange in wireless sensor networks," *IEEE Access*, 2024.

29. M. G. Moghaddam, A. A. N. Shirehjini, and S. Shirmohammadi, "A WiFi-based method for recognizing fine-grained multiple-subject human activities," *IEEE Transactions on Instrumentation and Measurement*, vol. 72, pp. 1–13, 2023.

30. S. Mekruksavanich and A. Jitpattanakul, "Biometric user identification based on human activity recognition using wearable sensors: An experiment using deep learning models," *Electronics*, vol. 10, no. 3, p. 308, 2021.

Synopsis_WSN_updated 23-12-2025.docx

Chanakya National Law University

Document Details

Submission ID

trn:oid:::3618:125058024

Submission Date

Dec 23, 2025, 4:47 PM GMT+5:30

Download Date

Dec 23, 2025, 4:49 PM GMT+5:30

File Name

Synopsis_WSN_updated 23-12-2025.docx

File Size

146.8 KB

29 Pages

6,133 Words

36,541 Characters

11% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text

Match Groups

76 Not Cited or Quoted 11%
Matches with neither in-text citation nor quotation marks

0 Missing Quotations 0%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

8% Internet sources
4% Publications
9% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Match Groups

76 Not Cited or Quoted 11%
Matches with neither in-text citation nor quotation marks

0 Missing Quotations 0%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

8% Internet sources
4% Publications
9% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Submitted works	Citrus Community College on 2015-02-10 — 3%
2	Internet	www.mdpi.com — <1%
3	Internet	dokumen.pub — <1%
4	Internet	files01.core.ac.uk — <1%
5	Internet	www.ijirset.com — <1%
6	Internet	aspe.hhs.gov — <1%
7	Internet	link.springer.com — <1%
8	Internet	www.divai.sk — <1%
9	Internet	download.bibis.ir — <1%
10	Publication	Jeon, Eun Som. "Knowledge Distillation with Geometric Approaches for Multimod... — <1%

11 Submitted works
Dr. B R Ambedkar National Institute of Technology, Jalandhar on 2023-04-02 <1%

12 Submitted works
University of Nottingham on 2025-09-12 <1%

13 Internet
www.jetir.org <1%

14 Submitted works
American Public University System on 2025-04-06 <1%

15 Publication
G. Arunsankar, B. Gopi, Rajeshkumar Sampathrajan, S. Sasikala, A. Vanathi, C. Sri... <1%

16 Internet
www.preprints.org <1%

17 Submitted works
University of Teesside on 2024-12-29 <1%

18 Submitted works
Coventry University on 2025-12-15 <1%

19 Submitted works
University of Hertfordshire on 2024-08-19 <1%

20 Internet
www.nature.com <1%

21 Publication
"Advanced Information Networking and Applications", Springer Science and Busi... <1%

22 Submitted works
Anna University on 2024-06-08 <1%

23 Submitted works
Liverpool John Moores University on 2023-04-05 <1%

24 Submitted works
Saintgits College of Engineering on 2025-10-26 <1%

25 Submitted works
Swiss School of Business and Management - SSBM on 2025-12-01 <1%

26 Submitted works
University of Kent at Canterbury on 2023-04-06 <1%

27 Internet
americaspg.com <1%

28 Internet
conf.papercept.net <1%

29 Internet
digibug.ugr.es <1%

30 Internet
norma.ncirl.ie <1%

31 Internet
peerj.com <1%

32 Internet
sciresjournals.com <1%

33 Internet
wjaets.com <1%

34 Internet
www.epj-conferences.org <1%

35 Internet
www.ijsce.org <1%

36 Submitted works
De Montfort University on 2023-09-01 <1%

37 Publication
Sepp Hochreiter, Jürgen Schmidhuber. "Long Short-Term Memory", Neural Comp... <1%

38 Publication
Atiqur Rahman Ahad, Sozo Inoue, Guillaume Lopez, Tahera Hossain. "Human Acti... <1%

39 Submitted works

Brunel University on 2024-01-18 <1%

40 Publication

Nishanth Adithya Chandramouli, Sivaramakrishnan Natarajan, Amal H. Alharbi, S... <1%

41 Publication

Sakorn Mekruksavanich, Anuchit Jitpattanakul. "Deep Learning Networks for Co... <1%

42 Publication

Jungpil Shin, Najmul Hassan, Abu Saleh Musa Miah, Satoshi Nishimura. "A Compr... <1%

IEEE

IDCIoT

REVA UNIVERSITY

3rd International Conference on
Intelligent Data Communication Technologies and Internet of Things
(IDCIoT-2025)

5-7, February 2025 | Bengaluru, India

Certificate of Presentation

This is to certify that

Pallavi

has successfully presented the paper entitled

IoT-Based Women's Safety Monitoring in Educational Campuses Using WSN and Deep Learning

at the
3rd International Conference on
Intelligent Data Communication Technologies and Internet of Things (IDCIoT-2025)
organised by School of Computer Science and Engineering, REVA University,
Bengaluru, India during 5-7,February 2025.

Session Chair

Dr. Syed Muzamil Basha
Conference Chair

Dr. Ashwinkumar U.M
Director

XPLORE COMPLIANT ISBN: 979-8-3315-2754-9